RPTR MCGHEE

EDTR CRYSTAL

END THE TYPHOONS: HOW TO DETER BEIJING'S CYBER ACTIONS
AND ENHANCE AMERICA'S LACKLUSTER CYBER DEFENSES
Wednesday, March 5, 2025
House of Representatives,
select committee on the Strategic Competition Between
the United States and the Chinese Communist Party,
Washington, D.C.

The committee met, pursuant to call, at 9:15 a.m., in Room 390, Cannon House Office Building, Hon. John Moolenaar [chairman of the committee] presiding.

Chairman Moolenaar. The select committee will come to order.

As we speak, the Chinese Communist Party is waging a full-scale cyber war against the American people, an attack on our security, our infrastructure, and our way of life.

The CCP has targeted the grids that power our homes, the facilities that treat our water, and the hospitals that care for us as part of their cyber warfare on the American people.

Last year a Chinese hacking group called Salt Typhoon infiltrated America's leading telecommunications firms, including Verizon and AT&T. This group dedicated vast resources to accessing our most sensitive data -- information found on our phones and wireless devices, including likely listening to phone calls conducted by President Trump and Vice President Vance.

This is not an isolated incident. Another Chinese hacking group, Volt Typhoon, has been working to position itself inside our critical infrastructure. According to intelligence officials, Volt is preparing to disrupt or destroy vital services in the event of a crisis over Taiwan.

It is clear Xi Jinping's goal is to sabotage our way of life when the time is right for his regime. These cyber operations are part of a broader coordinated effort by the Chinese Communist Party targeting everything from water utilities in Hawaii, to oil pipelines on the West Coast, and even the Texas power grid.

The party's goal is clear: to undermine the very systems that keep this country running.

We must understand that this isn't just a cyber threat. This is part of the CCP's larger strategy to destroy the American way of life.

As we have seen with the deliberate flooding of fentanyl into our communities, the CCP will stop at nothing, even if it costs the lives of hundreds of thousands of Americans, to advance its goals of global dominance.

Just last fall, the ranking member and I warned that Chinese infiltration of our critical infrastructure is like a loaded gun aimed directly at the American people.

Today that gun is aimed and ready to fire.

For example, CCP-linked companies, like DJI and Autel, control 85 percent of the domestic drone market, while 80 percent of U.S. ports rely on cranes supplied by ZPMC, another PRC entity.

With Volt Typhoon, the Chinese Communist Party is prepared to pull that trigger the moment it suits the interests of Xi Jinping and his regime.

The CCP views all forms of warfare -- cyber, economic, ideological, and military -- as different tools to achieve the same goal: global domination through the defeat of its enemies.

The CCP has never made any distinction between civilian and military targets in warfare, cyber or any other. To ignore aggression in one field is to invite aggression in every other.

There must be consequences for Chinese cyber operations that endanger the American people and our national security.

CCP-linked companies that enable cyber warfare against America, either through direct complicity or by more subtle means, such as providing back doors, should not be allowed anywhere near our critical infrastructure.

Through military-civil fusion, the CCP has mobilized every sector under its control to wage cyber warfare against America. To combat that, we need to work together.

There is one glimmer of good news: The Trump administration has already shown a willingness to take a more aggressive stance in cyberspace.

National Security Advisor Mike Waltz and key members of the National Security Council have made clear America must be ready to use its offensive cyber capabilities to deter, disrupt, and destroy adversaries that target our security.

The National Security Council is signaling that America is no longer only playing defense. We are actively engaging to erode our adversaries' cyber capabilities.

This commitment to offensive cyber operations is aligned with one of the end goals of the select committee: protecting the American people from CCP interference and ensuring the safety of our critical infrastructure.

We resolve to push back against China's malign actions and prevent further encroachment into our digital ecosystem.

We must work with the White House, the private sector, and our allies around the world to continue educating on the dangers the CCP cyber warfare poses to their security and how they can protect themselves.

We are grateful to have with us today three excellent witnesses who will provide context on the CCP's cyber threat and highlight measures we can take to defend ourselves.

In 2014, Xi Jinping told the CCP that without cybersecurity there can be no national security. This is a rare instance where I have to agree with the General Secretary.

American cybersecurity is American national security, and if we fail to hold Beijing accountable, the CCP's cyber warfare will merely be the prelude to a military assault on the American people and our allies.

And on that note, I would like to yield to Ranking Member Krishnamoorthi for his opening statement. I now recognize Ranking Member Krishnamoorthi.

[The statement of Chairman Moolenaar follows:]

******** COMMITTEE INSERT ********

Mr. Krishnamoorthi. Thank you, Mr. Chair.

This picture is a picture of a GPS tracking bracelet. The U.S. Government puts them on people convicted of serious crimes so we can see where these criminals are at all times.

But imagine if China had the very same capability to track and surveil our location, but not just for criminals, but for potentially every single American.

Last year Federal authorities confirmed that China, through a hacking group known as Salt Typhoon, broke into the networks of nine major telecom providers. That access allowed the CCP to, in the words of one former official, quote, "geolocate millions of individuals and even record phone calls at will."

If the CCP was listening in on this Congress, they'd know the bills we were going to introduce, the investigations we were going to launch, and most importantly, the actions they needed to take to evade consequences.

I want to let the enormity of that sink in for a second.

Salt Typhoon was one of the worst hacks in American history, a truly unprecedented intelligence breach. And it comes just one year after this committee held a hearing on Volt Typhoon, an equally devastating hack where we learned that China has prepositioned vulnerabilities in our critical infrastructure that they could deploy to disrupt them in time of conflict.

These are hardly isolated incidents. From the theft of millions of Americans' security clearance records in 2015, to the hack of the Treasury Department just this past December, we're essentially an open book for Chinese intelligence agencies.

It's time to slam that book shut and get the CCP out of our networks once and for all.

First, we're going to bolster our defenses and invest like never before in our Nation's cybersecurity.

An obvious place to start is "edge devices," a fancy word for the hardware that serves as the entry point for a network, like a WiFi router.

There is a common thread between Volt Typhoon and Salt Typhoon, and it's the use of edge devices to break into our systems.

Second, we need to hone in on telecom.

Just yesterday the chairman and I sent letters to China Mobile, China Unicom, and China Telecom about their remaining operations in the U.S.

As Reuters recently put it, these firms could exploit access to American data through their U.S. cloud and internet services by providing that data to Beijing.

But we can't stop there. American telecom companies should also need to meet rigorous cybersecurity standards. Just like with oil pipelines after the Colonial Pipeline attack, Salt Typhoon is a wakeup call that we can't just rely on telecom companies to police themselves.

Third, we need to increase our cyber talent pipelines. We have 1.5 million cybersecurity workers currently, but we need 2 million. That's a 500,000-person gap and something we need to work on.

Fourth, we need to hold the CCP accountable. Some people call this "defending forward." It means imposing costs on the CCP each time they attack us.

When Xi Jinping decides whether to launch another attack, he needs to ask himself whether the costs are worth the benefits.

With the full force of NSA, CISA, and other cyber experts, we need to make China think twice. This is only going to become more important as AI makes cyber attacks more effective and harder to detect.

Because of that, I'd like to close with a message created by AI so you can see the power of this technology for yourself.

[Video shown.]

Mr. Krishnamoorthi. Thank you, deepfake Raja.

And thank you to our witnesses for joining us today.

Thank you.

Chairman Moolenaar. Thank you very much, and it's great to have the real Raja here with us today.

If any other member wishes to submit a statement for the record, without objection, those statements will be added to the record.

I'd like to go to our witnesses now.

I want to first introduce Mr. Rob Joyce, former special assistant to President Trump and acting Homeland Security Adviser. Mr. Joyce has defended Americans over the course of more than three decades at the National Security Agency. Mr. Joyce has loyally served Presidents of both parties, and I look forward to hearing his insights on the threat facing our Nation.

Welcome.

Our second witness is Dr. Emma Stewart, who currently serves as the chief power grid scientist for national and homeland security at Idaho National Laboratory, having previously worked as their chief power grid scientist and research strategist.

Welcome.

Dr. Stewart brings more than a decade of work protecting the power grid from Chinese hackers who have repeatedly targeted it for infiltration in the event of a conflict, sabotage.

Finally, we are joined by Laura Galante. Ms. Galante helped lead the intelligence community's response to cyber warfare threats at the Office of the Director of National Intelligence after more than a decade advising private and public sector clients. We're proud to have her with us today as well.

I want to welcome all three of you.

And if you could please stand and raise your right hand, I will now swear you in.

[Witnesses sworn.]

Chairman Moolenaar. Let the record show that the witnesses have answered in the affirmative.

And thank all of you for joining us this morning.

Mr. Joyce, now I would like to recognize you for your opening remarks.

TESTIMONY OF MR. ROB JOYCE, FORMER DIRECTOR OF CYBERSECURITY, NATIONAL SECURITY AGENCY; DR. EMMA M. STEWART, CHIEF POWER GRID SCIENTIST, NATIONAL AND HOMELAND SECURITY, IDAHO NATIONAL LABORATORY; AND MS. LAURA GALANTE, FORMER DIRECTOR OF THE CYBER THREAT INTELLIGENCE INTEGRATION CENTER, OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE

TESTIMONY OF ROB JOYCE

Mr. Joyce. Honorable Chair, Ranking Member, and distinguished members of the committee, thank you for the opportunity to appear here today.

The PRC is conducting a comprehensive campaign against the United States and our current defenses are not keeping pace. Chinese state hackers have prepositioned malware within our power grids, pipelines, water treatment plants, and other critical infrastructure. They tapped into our telecommunications to spy on us. They stole the innovations of technological research and breached the cloud systems holding government emails. They even unfairly exploit our open markets to achieve a growing advantage inside the technology we rely on for our communications.

After a decade of using cyber to steal our industrial and military secrets and advantages, they've evolved to a far more threatening penetration of our Nation's infrastructure. They run cyber operations deliberately intended to create "societal panic" at the time of escalating tensions.

Planning cyberterrorism is a direct threat to our national security and economy. The PRC is not only using cyber operations to their advantage, they're undercutting our market to deliver their Chinese-controlled technologies into our homes, raising significant national security concerns.

TP-Link, the world's largest manufacturer of commercial WiFi and home routers, has grown to at least 60 percent of the U.S. retail market for WiFi systems and SoHo routers compared to about 10 percent of the market at the start of 2019.

How have they achieved this miraculous growth? They appear to be selling at price points below profitability to drive out our Western competition.

As of August 2024, TP-Link captured nearly 80 percent of the U.S. retail market for mesh systems running on WiFi 7, which is the newest WiFi specification in existence.

TP-Link routers were among the various brands exploited by Chinese state-sponsored hackers in the massive Volt, Flax, and Salt Typhoon attacks.

Imagine these routers in the homes and businesses across America as a PRC platform to launch society-panicking cyber attacks during the invasion of Taiwan.

We cannot have the software for prolific devices be written, updated, and controlled by a Chinese company. By law, such a company is subject to the direction of the PRC intelligence apparatus. This is a threat we cannot ignore.

I know this hearing today isn't simply about the problems we face. It's important for us also to discuss the solutions that will keep us safe.

There are three pillars of work we must focus on.

First, we must improve our tools to deter those PRC actions.

Deterrence is not an abstract concept. It requires making clear to everyone in the chain of command, from the individual hackers to the military generals in the Politburo leadership, that the costs of these cyber operations outweigh any potential benefits.

And while the strengthening of our cyber defenses is essential, this alone will not change their behavior.

No single approach will achieve effective deterrence. Instead, we need a comprehensive campaign that imposes costs across multiple dimensions.

This integrated arsenal should include offensive cyber operations to disrupt their capabilities, targeted economic sanctions, public indictments, coordinated international law enforcement actions, diplomatic pressures, export control, and intelligence sharing with industry and our allies.

Overall, we must include high-level political engagement to establish clear expectations for acceptable behavior online coupled with concrete demonstrations that violations will have meaningful consequences.

Second, we need stronger defenses. Too often attackers exploit well-known vulnerabilities that remain unpatched.

Industry also leaves too many flaws in the software we rely on. There are certainly levers that can drive more security into the ecosystem and we must use them. This includes eliminating TP-Link's footprint from our Nation and ensuring other PRC capabilities are not enabled in our infrastructure.

Part of the defense is also having expertise and capacity in the government. I want to raise my grave concerns that the aggressive threats to cut U.S. Government probationary employees will have a devastating impact on the cybersecurity and our national security.

At my former agency, remarkable technical talent was recruited into developmental programs that provided intensive unique training and hands-on experience to cultivate vital skills.

Eliminating probationary employees will destroy a pipeline of top talent essential for hunting and eradicating PRC threats.

Even if the positions are not eliminated, the pervasive uncertainty and doubt in the current environment is forcing them to seek and secure opportunities for their families outside national security. We need this talent to win in competition and conflict.

Finally, assuming our adversaries continue to come at us and our defenses improve, we must plan to be resilient. We must ensure cyber attacks have limited impact, quick recovery, and minimal disruption. There are mitigations that must be made to reduce our exposure even when the hacks are successful.

I look forward to exploring these concepts during your questions. Thank you.

[The testimony of Mr. Joyce follows:]

******** COMMITTEE INSERT ********

Chairman Moolenaar. Thank you, Mr. Joyce.

Dr. Stewart, you may now proceed.

TESTIMONY OF EMMA M. STEWART

Ms. Stewart. Chairman Moolenaar, Ranking Member Krishnamoorthi, and members of the select committee, thank you for the opportunity to testify today on a topic critical to our national security.

My name is Emma Stewart, and I'm the chief power grid scientist at the Idaho National Laboratory. The work I perform is at the intersection of energy security, cybersecurity, and resilience. Our critical infrastructure research, development, and deployment efforts enable stakeholders to understand and mitigate the most consequential threats.

INL is one of 17 U.S. DOE national labs focused on building and testing more than 50 nuclear reactors in our full-scale test site. INL has developed a deep understanding of the operational technology and the cybersecurity engineering and processes needed to secure systems and provide critical function assurance.

It is with this knowledge I speak to you today about the threat we face from the CCP to the security of our energy delivery system.

The backbone of our society is energy, with the U.S. having the most complex, interconnected, and currently reliable electric grid in the world.

In the U.S. we enjoy the capability and flexibility of electricity at any time, to any level, as a foundation of our economy, which enables military missions, delivers clean water, provides medical resources, and supports innovation.

Over the past two years, we've heard from many qualified experts, Federal organizations, such as joint statements from DOE and DHS, and testimony about the threat the PRC imposes on our U.S. energy and other critical infrastructure sectors.

We face an unprecedented and multifaceted threat from these CCP actors given their ability and reported attempts to deliver cyber attacks which could catastrophically impact our ability to deliver power to U.S. citizens.

This is no longer a warning. It is happening now and will continue to happen without a strategic unified focus on defense and deterrence of these attacks.

The threat is demonstrated through the reports on Volt and Salt Typhoon which describe capabilities ranging from prepositioning access to our water and power networks with Volt, and intrusion, mass data collection, and espionage on our communications infrastructure with Salt.

While the attention has shifted recently to Salt Typhoon, the dangers that were presented by Volt Typhoon's prepositioning should not be understated or forgotten. This effort was not just about data collection. It was about gaining a foothold in many of our critical infrastructure controls.

Volt and Salt Typhoon could be referred to as intrusions from the back door of our country, leveraging known vulnerabilities and equipment. We must close those doors, remediate, and detect future evolutions rapidly.

We must also urgently address that which could be referred to as a front door threat, which is the PRC dominance of our supply chain with fundamental control layers, hardware, and power electronics that power our networks.

A recent study sponsored by the DOE Office of Cybersecurity, Energy Security, and Emergency Response, CESER, analyzed key manufacturers in the battery energy storage systems space and evaluated the impact of the integration of high volumes of battery storage from PRC manufacturers across the country.

The study revealed a complex web of manufacturers, asset owners, and integrators, indicating the challenge of untangling the supply chain from raw material to finished product through a 20-year strategy to acquire IP, expand manufacturing, and flood the market.

PRC manufacturers today dominate this field with at least 70 percent of manufacturers being PRC based and over 90 percent having critical components from the PRC.

When discussing solutions, the elephant in the room with PRC-dominant supply chains is Rip and Replace. It's a common recommendation for Chinese components. While effective in single-vendor threats, removing all of these technologies right now would harm our resilience and hinder the growth of the U.S. supply chain.

The study prioritized commercial and Federal solutions and recommendations ready for immediate implementation to help solve this threat now. These measures protect, defend, and enable secure operation despite malicious supply chain actions, enabling strategic hunting and removal of threats like Volt Typhoon.

However, no single solution exists to defeat this threat. We can repatriate critical component software and invest in a secure U.S. and allied manufacturing base that requires a focused, urgent deployment strategy.

With the help of the national labs, DOE CESER and the DOE Grid Deployment Office are already piloting this kind of assistance, hunting adversaries and implementing those controls to remediate the issue in the battery supply chain in particular, promoting the secure operation.

One key solution in the portfolio is the use of cyber-informed engineering to enable, design, and effectively secure around and operate through the most consequential events.

This portfolio has enabled us to work with all levels of asset owners, small to large, providing strategic operational and engineering solutions and prevent those most consequential cyber events.

This work is not done. It leads to a second set of challenges and solutions, which is our ability to deploy, defend, and have deterrent capabilities.

We might have the technology to remediate and repatriate, but we do not have a coordinated deployment strategy and market forces are not enabling effective portfolios to be built or customized.

Our strategic defensive capabilities for the OT space are currently split into factions between national labs, private industry, and Federal entities.

What I believe is needed is a task force with coordination and unification of our deployable resources with strategic leads, Federal funding incentives, and State backing, along with streamlined authorities to actually perform the remediation actions we need to do. It would provide critical backup to those asset owners who urgently need the support to take action against Volt Typhoon and others.

To summarize, we have solutions. We need to use them fast and surgically to excise the most consequential and simultaneous threats from our networks to our energy delivery system.

I appreciate the opportunity to testify today, and I look forward to your questions.

[The testimony of Ms. Stewart follows:]

******** COMMITTEE INSERT ********

Chairman Moolenaar. Thank you, Dr. Stewart.

Ms. Galante, the floor is yours.

TESTIMONY OF LAURA GALANTE

Ms. Galante. Good morning, Honorable Chair, Ranking Member, and esteemed members of the committee. I'm Laura Galante. I most recently served as the director of the Cyber Threat Intelligence Integration Center and the intelligence community's cyber executive for the Office of the Director of National Intelligence.

Today I'm going to focus my remarks on one of the core root causes for how Chinese actors are able to penetrate so much of U.S. networks and critical infrastructure.

Back in fall 2024 U.S. media reported that numerous U.S. telecoms and other wireless communications companies were the victims of an extensive Chinese-sponsored intelligence operation.

This operation has been dubbed Salt Typhoon. The Chinese actors have breached multiple layers of at least nine major U.S. telecoms networks. This gives the PRC, the Chinese Government, wide access to U.S. mobile communications across carriers and across different wireless communication technologies.

This operation is the most extensive and most consequential cyber espionage operation ever launched against the U.S. The targets of this operation, the U.S. telco providers, secure some of the most complex and highly valued networks and infrastructure.

In 2023 the then-Director of National Intelligence warned that, quote, "China's cyber espionage operations have included compromising telecommunications firms, providers of managed services and broadly used software, and other targets potentially rich in follow-on opportunities for intelligence collection, attack, or influence operations."

Telecom providers operate multiple technology stacks, from the literal physical "pipes" of the internet up to the customer-facing services like texts and calls.

Telecommunications technologies have dramatically evolved over the last 20 years, and many of the companies that we know today have also had various acquisitions that have put together different systems. These companies still maintain those legacy networks and technologies.

Despite the telecom's significant internal cybersecurity operations, detecting Salt Typhoon's compromise has required an extensive joint government-industry response. The U.S. Government has issued a series of advisories and guidance to help companies identify whether they are Salt Typhoon victims.

I'd like to shed some light on the people behind these breaches.

This is a group of contractors who work for China's Ministry of State Security, similar to the CIA in U.S. terms.

In January, the Department of Treasury sanctioned Sichuan Juxinhe Network Technology Co., LTD., citing their "direct involvement in the exploitation of these U.S. telecommunication internet service provider companies. The MSS has maintained strong ties with multiple computer network exploitation companies, including Sichuan Juxinhe."

Who is the MSS?

The Ministry of State Security, among other functions, handles the Chinese counterintelligence, espionage, and political security functions.

The MSS, like other state Chinese cyber operators, relies on a network of companies that perform research and development tasks that serve as the basis for compromising vulnerabilities in network configuration and security products that are used in the U.S.

These companies frequently change names, they alter their corporate structures, they take other steps to avoid scrutiny and detection.

This ecosystem, sometimes called "hackers for hire," of Chinese IT and cybersecurity contractors remains largely intact and undeterred by U.S. sanction efforts and by the widely publicized 2024 leak of the inner workings of one of those contractors called I-Soon.

This Salt Typhoon operation against U.S. telcos demonstrates that this outsourced "hack for hire" model, where contractors can achieve major espionage objectives for the Chinese state against complex high-value victim networks, shows how China is able to scale these operations against the U.S.

It provides a competitive marketplace, a business network, if you will, for these exploitation capabilities and outsources some of the most sensitive target development and operations like those against U.S. companies.

This, in effect, minimizes the risk of exposing the larger state espionage and attack plans that China has.

Salt Typhoon's success in compromising multiple parts of the U.S. telecommunications architecture builds on over a decade of bulk as well as targeted cyber espionage operations against the U.S.

In 2015, the Office of Personnel Management's databases were hacked. They had over 21 million former and current government employees' Social Security numbers, addresses, and data points.

In 2023 China was also able to successfully breach the Department of State and Microsoft in order to collect on the communications of senior U.S. officials involved in U.S. China policy.

These are just a few of the examples of the personal data and operations that China has used against us.

Where is this going finally?

To understand where the PRC is going to take this capability, we need look no further than their own domestic surveillance apparatus that they have put in place against the Chinese people.

The DNI put it succinctly in 2023: "China leads the world in applying surveillance and censorship to monitor its population and repress dissent."

As the PRC refines its tools and methodologies domestically, particularly with the application of their recent AI advances, we should expect them to harness and deploy these capabilities against us, our allies, and other nations critical of China.

Thank you. I look forward to your questions.

[The testimony of Ms. Galante follows:]

******** COMMITTEE INSERT ********

Chairman Moolenaar. Thank you, Ms. Galante.

Thank you all for your testimony.

And now we'd like to move to questions. And I'd like to begin by talking about the concern of the potential for a cross-strait conflict with Taiwan and the very real threat of Chinese cyber warfare against the United States.

I wondered if you could, Mr. Joyce, talk about, in the event of a Chinese military operation, how prepared and what would we expect in a Chinese cyber attack?

Mr. Joyce. Mr. Chairman, I think it was a hearing that this committee held where the director of NSA, FBI, CISA, and the National Cyber Director testified about the Volt Typhoon threat.

And in that they talked about the intent of the Chinese to, one, disrupt our military transport capabilities to move into the theater. So we would have to transport an enormous amount of people and materiel.

And you can imagine that the computers that plan and support the DOD, both in civilian infrastructure and in the government, are an important aspect to our success in being able to mount that defense.

So the Chinese would look to disrupt those capabilities to move, organize, and get to the theater of conflict.

The second thing they'd do, though, is they would want to cause the American people to be disrupted and concerned by cyber attacks against our critical infrastructure here in the U.S. so we would turn inward and have that societal panic where we wouldn't be interested in a fight on the other side of the world. We'd be dealing with messes here.

So they're prepositioned in things like rail, transport, ports, air, our airlines, and others, the electric grid, the water supply, so that they could create that disruption here in the U.S. and cause us to not have the will to get into that fight.

Chairman Moolenaar. Thank you.

And, Dr. Stewart, it seems that our cyber defenses are not up to standard where we'd want them to be.

What can be done -- you mentioned the prepositioning when it came to Volt Typhoon -- when you think of this kind of aggressive action, how do we bring our cyber defenses up to a satisfactory level?

Ms. Stewart. My expertise is mostly in the power grid, so talking about our utilities and what they need to improve their cyber defenses at the moment.

There has been a lot of work through various programs -- one of them is the rural municipality utility cyber program also -- to provide them funding, access to resources, and people essentially to help them improve their defenses.

At this point we still do not have enough people and enough resources going to them, and that requires funding and capabilities as well.

We are deploying things to help them solve these things. We have the tools. We need people and capabilities going out there and helping them remediate those actions together, unified forces essentially that take the best of our abilities and help put them in the right, most consequential places as well to help them build those defenses.

Chairman Moolenaar. Okay. Thank you.

Mr. Joyce, in your testimony you spoke about TP-Link and the threat that it presents.

Why should consumers care about TP-Link? How would they even be aware -- you know, you hear about -- I heard from someone recently who said his mother had a router, a TP-Link router. I mean, how would people even know this? How concerned should we be? You mentioned, I think, 60 percent of the market is TP-Link?

Mr. Joyce. Yes, sir.

So those devices are labeled and branded TP-Link. So by looking at your home WiFi router you can understand if you have a TP-Link router.

The concern is the Chinese cyber operations need to come all the way from China out to their victims in the U.S., the critical infrastructure inside the U.S. And most of our cyber defenders know that when something knocks on their front digital door from China, they need to look at it very closely.

But by hacking these WiFi routers, they can come through the internet, emerge in our homes and our businesses, and then move onward to those targets and have a much better reputation, because it looks like work from home or it looks like the connections they would expect from their customers. So they can't block those.

So by having these routers in your home, you are exposing the attack surface of the U.S. critical infrastructure for the types of operations you asked about in your first question, sir.

So we need to all take action and replace those devices so they don't become the tools that are used in the attacks on the U.S.

Chairman Moolenaar. Is there any action the Commerce Department should utilize to take action against TP-Link?

Mr. Joyce. Yes, sir. Congress has the authority on a national security basis to block and bar those devices from sale in the U.S. And I understand they are working on that today, and I would encourage everybody to move swiftly and quickly on that action.

Chairman Moolenaar. Thank you very much.

And I'd now like to recognize the ranking member for five minutes of questions.

Mr. Krishnamoorthi. Thank you, Mr. Chair.

Thank you to the witnesses.

China is the world's foremost hacker, as this visual displays.

Ms. Galante, as you can see on the chart behind me, between 2000 and 2020, the Chinese Government was responsible for more state-sponsored hacks to steal data than Russia, North Korea, and Iran combined, correct?

Ms. Galante. That's correct.

Mr. Krishnamoorthi. But numbers alone do not tell the whole story. In fact, one of our worst hacks in our Nation's history, Salt Typhoon, was only discovered a few months ago.

This Chinese state-sponsored hacking group penetrated at least nine major telecom companies, as we've mentioned before.

Mr. Joyce, according to news reports, the CCP had access to call logs, unencrypted texts, audio messages, geolocation data, and even the private portals of law enforcement for court-ordered monitoring, correct?

Mr. Joyce. Yes, Congressman, that's my understanding.

Mr. Krishnamoorthi. And, Ms. Galante, this kind of data could be used for blackmail or coercion by the CCP, right?

Ms. Galante. Yes, in addition to other purposes.

Mr. Krishnamoorthi. The good news is that encrypted messages and calls are much more secure. I know when I communicate with my staff, we actually use Signal, as you can see here. It's a free encrypted app to keep our messages and calls protected.

So, Mr. Joyce, if there's one thing all of us, every single American can do right now to protect ourselves, it's to use encrypted messaging platforms such as Signal, right?

Mr. Joyce. Yes, Congressman. I use Signal as well.

Mr. Krishnamoorthi. Okay. Well, maybe we'll Signal each other.

Okay. Let's turn to the next topic.

Individual actions alone aren't enough. To tackle the CCP cyber threat head-on, we need to reimagine our supply chains and invest in cybersecurity like never before.

This is particularly true with regard to what are called "edge devices." To put it simply, these are things like routers that connect a device to a network.

According to public reports, Salt Typhoon broke into our telecom networks by exploiting software vulnerabilities tied to edge devices, just like Volt Typhoon compromised edge devices in our critical infrastructure.

Ms. Galante, it's clear that we need minimum cybersecurity standards for edge devices, correct?

Ms. Galante. Yes. These edge devices are frequently the way that the Chinese are able to access and get into core networks that we've discussed.

Mr. Krishnamoorthi. So we just talked about TP-Link. The chairman mentioned that.

And here is a TP-Link router, Chair. I actually brought one here.

You can actually buy one of these things for $20 online. But don't use this, okay? Don't put it in your critical infrastructure. And as the chairman mentioned, I don't have one at home either. It's not a good idea.

Let me turn to my final topic.

As individuals, we can use encrypted messaging apps and safer routers to protect our privacy. And as Congress, we can require telecom and critical infrastructure companies to up their game. But really the biggest question is: How do we get the CCP to stop?

So, Mr. Joyce, there's no such thing as perfect cybersecurity, and it feels like the CCP is going to just keep hacking until the costs exceed the benefits, right?

Mr. Joyce. Yes, Congressman.

Mr. Krishnamoorthi. So it seems to me like step one is we have to figure out how to attribute hacks back to their sources, such as the CCP, but step two is imposing consequences.

We've tried having DOJ indict CCP hackers, as this poster shows behind me. We've tried sanctions. These efforts are important, but they don't seem to be enough.

The most important tool, in my opinion, is something that Cyber Command calls "defending forward." And to ask a question about this, I'm going to turn back to the deepfake of myself, which we met during my opening statement, to pose a question to our witnesses.

Mr. Krishnamoorthi. [Video of deepfake: "With the rise of generative AI, the technology used to produce deepfakes like the one you are watching right now, cyber attacks against America are going to get even bolder and more brazen.

"Mr. Joyce and Ms. Galante, to deter the CCP and impose serious consequences on them, we need to hack back. Isn't that correct?"

Mr. Joyce. So my answer is a strong "yes and." It's not just "hack back," but it is the entirety of a comprehensive plan that ensures they understand that hacks come at a cost.

Mr. Krishnamoorthi. Ms. Galante?

Ms. Galante. I agree with that. And we also need to go after some of the core companies and enablers that are behind the Chinese Government's system.

Mr. Krishnamoorthi. Yes. I think we should hack back the hackers.

And I'm going to say something very provocative. I think that we should also consider potentially enlisting private sector actors to hack back at the hackers. I'm going to get in a lot of trouble for saying that, but I think you have to sometimes use fire against fire.

So thank you. And I yield back.

Chairman Moolenaar. Thank you.

I'd like to call on Representative LaHood.

Mr. LaHood. Thank you, Mr. Chairman.

I want to thank the witnesses for your valuable testimony here today.

Mr. Joyce, good to see you again.

I also serve on our House Intelligence Committee and I chair our NSA and Cyber Subcommittee. And so I appreciate the candor and sincerity of your testimony today.

As has been referenced regarding China, under Xi Jinping's leadership CCP leaders have consistently expressed their public intention in becoming a cyber superpower. And I'm going to ask you, Mr. Joyce, about that in a second.

And their official government view is that cyberspace is a venue for international strategic competition and how they win that strategic competition.

Of course, that pertains to national security. It pertains to economics. It pertains to technology.

The CCP's own cyber policymaking process has placed an emphasis on using cyber espionage for illegitimate economic advantage and refusing to abide by a set of principles of international law in the digital domain. They play by a different set of rules and standards that every other industrialized country in the world abides by.

So, Mr. Joyce, maybe my first question, if they are not a cyber superpower now in terms of their actions, what does that look like if they're able to achieve that?

Mr. Joyce. I believe China is approaching a peer status in cyber. If you look back 10, 15 years, they were not skilled and not a significant power, but they have a couple of things that have benefited them.

One, they have mass. They have quantities of intelligence, military, and commercial entities on a scale that dwarfs anything we in the West have.

Two, they're gaining experience just through the sheer volume of operations they're doing against the U.S. and our Western allies. They get better through experience.

And then, third, they've been willing to try things and learn from their mistakes. And so they continue to advance, moving from espionage and theft into that prepositioning and the capability to do attack and disruption.

Mr. LaHood. Thank you.

Our new CIA Director, John Ratcliffe, in his confirmation hearings talked and advocated for more aggressive offensive actions to counter the CCP's growing influence around the world. Kind of a general statement. And I believe this approach needs to be extended to the cyber domain specifically to better allow the U.S. to leverage cyberspace capabilities and to safeguard our national security.

Mr. Joyce, you may be aware, last week the cybersecurity company CrowdStrike released their global threat assessment, and it's really alarming. They found a 150 percent increase from 2023 to 2024 in PRC-related cyber threats across all 23 sectors that they track, ranging from the defense industry to financial services to telecommunication and everything in between.

So what's your assessment in why Chinese cyber actors are increasing their cyber espionage and attack tempo at such a significant pace?

Mr. Joyce. So my assessment is they're increasing because it's yielding results. They're getting intelligence. They're getting critical financial and proprietary information that lets them advance their economic interests. And they're doing it because it strategically is advantaging them, both in the military and intelligence side.

So they're doing it, frankly, because it continues to be successful and there is no cost to them for this effort.

Mr. LaHood. In terms of the threat that they face, do you have any suggestions or give us any optimism on the direction the U.S. is currently headed?

Mr. Joyce. Yeah. My belief is the dials need to be set to 11. That was my comment earlier that it's a "yes and," offensive cyber, but also diplomatic messaging, the investment in the operations.

Now is not the time to dial back on our cybersecurity capabilities, but put our foot down so that we can generate the intelligence that enables the operations to push back.

I'd ask you, too, when have you ever seen a diplomatic expulsion for a cyber event. We do that routinely when people spy on the U.S. We do that routinely when there's some sort of diplomatic misstep. We don't use it in the cyberspace.

And that shows me we don't use all the tools of national power. We have tremendous leverage in economic and commercial space. We don't use that to push back for cyber intrusions. We need to use everything on a scale that turns the dial to 11.

Mr. LaHood. Thank you. I yield back.

Chairman Moolenaar. Thank you.

Representative Carson.

Mr. Carson. Thank you, Chairman.

The U.S.-China Business Council consists of over 270 companies with ties to China.

What are the biggest cybersecurity and operational challenges U.S. companies face in China? And how can Congress and the administration support businesses navigating China's cyber laws while protecting our national cybersecurity interests?

Ms. Galante. One of the key concerns that these U.S. companies will have as they look at doing business in China is the potential for espionage on their own business networks.

We've seen for over now almost two decades a focus from a variety of different actors in the Chinese Government to go after key intellectual property and then funnel that IP into state-owned enterprises in China. That mechanism is well honed and proved out against U.S. companies.

In order to look for and build cybersecurity programs that will be able to detect the type of attacks and the type of espionage that we've been talking about today, these companies should employ robust measures that get in a program that includes identity management, that has patching and vulnerability identification and threat hunt activities at the core of it.

Mr. Carson. Under the Secure and Trusted Communications Network Act of 2019, the Rip and Replace Program was born.

How can Congress accelerate the Rip and Replace Program to ensure small telecom providers can fully transition away from high-risk Chinese equipment? And what additional measures should we consider to further protect U.S. telecom networks from espionage and cyber threats?

Ms. Galante. I think the discussion around TP-Link, the Chinese-owned manufacturer and creator of a dominant portion of the router market, is one of those key measures, identifying where there are products that Americans have in their own home networks or their businesses and being able to say those technologies need to be ripped and replaced.

We saw something similar with Kaspersky Labs. Commerce, the Department of Commerce last year issued that Rip and Replace or banned Kaspersky products from being used in the American commercial sector.

We need the same sorts of activities happening for TP-Link and for other home use and commercial grade technologies where China has an upper hand.

Mr. Joyce. Congressman, I would also offer the key action you can take is ensure that the programs are funded.

Most of these small telcos, they don't want Chinese infrastructure in their infrastructure either, but they have working devices and they can't afford to pull out the Chinese gear and put in trusted equipment. So please fund them.

Mr. Carson. Yes, sir.

Yes, ma'am.

Ms. Stewart. If we could also add that when we replace these devices, we need secure other devices as well to be in place. Sometimes when something is designed here, it doesn't mean it's necessarily the most secure, and we might still end up with the vulnerabilities in the system that are harming us at the moment.

So developing secure designs in this country would be also recommended from my perspective.

Mr. Carson. That's great.

Thank you. I yield back, Chairman.

Chairman Moolenaar. Thank you.

Representative Dunn.

Mr. Dunn. Thank you very much, Mr. Chairman.

I'd like to thank the witnesses as well for their testimony today.

And I want to make a special thank you to the chair and the ranking member for putting together such a brilliant panel of distinguished witnesses.

I think it's incumbent on us in Congress to effectively and decisively put a stop to the PRC's insidious cyber operations. As policymakers, we need to continue our efforts to establish comprehensive security strategies. I'm glad that you guys are actually including some "to do" messages to us today. We need that.

The recent cyber attacks on America's telecommunications infrastructure by PRC-sponsored hacking groups, Salt, Silk, Flax, Volt Typhoons, represent an alarming escalation in cyber operations.

The scope of these breaches is literally staggering. Salt Typhoon breached private text messages and phone calls of countless Americans. They potentially intercepted classified communications and documents from senior government officials. And even today the Federal agencies are still working to fully understand and eliminate the threats posed by these hacks.

Former Director of the FBI Christopher Wray identified that China steals more data than all other nations combined. The FBI cases of Chinese economic espionage surged by 1,300 percent over the last few years alone.

Even more concerning is China's strategic positioning within America's critical infrastructure. PLA-affiliated hackers have breached at least two dozen vital U.S. systems, from water utilities in Hawaii, power grids in Texas.

These intrusions of the Volt Typhoon campaign appear to be designed to disrupt our response capabilities during a potential simultaneous military campaign.

The U.S. must lead global efforts in cyber deterrence. I can tell you that NATO is also leaning in on this largely due to the experience that we've had with China.

The stakes are, in fact, high. A coordinated attack of these compromised systems could paralyze key industries.

As we've heard through our previous work with this committee, the PRC is laser focused and will stop at nothing to control and dominate and exacerbate any and every vulnerability.

We can no longer afford to be reactive. I think we need to be proactive, do something before they occur. And I'm encouraged by this administration's National

Security Council, which is poised to mobilize aggressive authorities to deter a cyber operation.

I look forward to working with my colleagues to ensure the protection of our national security assets and critical infrastructure and protect our private data.

Mr. Joyce, what are the most -- what are the worst current limitations of legal framework in terms of addressing cyber threats from China?

And in your testimony, you said that there are mitigations that must be made to reduce exposure. What are some of those mitigations you would have us do?

Mr. Joyce. Thank you, Congressman.

In terms of the authorities and the ability to act, one of the things that happens in cyberspace is there's ambiguity about borders. We have laws that are specific to geography, about the rights we have as Americans.

But the internet doesn't understand those borders. So the Chinese take advantage of those borders by coming and hacking those home routers and then going from the home routers to their victims.

The problem is now that once they're on that home router, they look like an American endpoint. And so the FBI is not able to quickly pursue that criminal act back into the network.

And the Chinese understand that. They use our domestic position and domestic laws to launch the attacks from a position of protection.

So we have to look at that. How do we give the FBI the agility to chase these intrusions inside the U.S. while respecting Americans' privacy? But they need more agility, sir.

Mr. Dunn. Thank you for your response. It makes me want to take one of you home and have you look at my router.

Can you expand on what the societal panic -- you mentioned societal panic -- events could look like that the PRC is attempting to create in times of escalating tensions. Specifically, are we talking about another run on toilet paper or maybe something more important?

Mr. Joyce. Definitely more important.

I think you can look back, sir, at Colonial Pipeline when the gasoline supply to the East Coast was shut down and people were literally using plastic bags to get the last loads of gasoline and hoard those and save them. So it's not exactly toilet paper, but it is absolutely causing that kind of concern in supply.

Mr. Dunn. All of you have expertise we need. Please stay in touch with our chairman.

Thank you, Mr. Chairman. I yield back.

Chairman Moolenaar. Thank you.

Representative Tokuda.

Ms. Tokuda. Thank you, Mr. Chair.

In recent weeks we have seen the Trump administration fire at least 140 employees at the Cybersecurity and Infrastructure Security Agency, which President Trump himself established during his first term.

Hundreds more, as we know, may be let go, many of them holding critical cybersecurity roles and providing valuable technical experience despite the fact that they have only been working at the institution for a short time.

Dr. Joyce, in your written testimony, you express your grave concern with the elimination of probationary employees and the harmful impacts that this has on not just the immediate cybersecurity posture of our country, but our ability to attract the right talent, especially when you consider the fact that the threats are not ceasing to exist, and who knows how many other Salt Typhoons we have embedded in our system as we speak right now.

Dr. Stewart and Ms. Galante, do you concur with Dr. Joyce's concerns?

Ms. Galante. I think Mr. Joyce's concerns about the firing and also the diminution of the Federal workforce on cybersecurity is a core concern.

I'll also say that with CISA in particular, the work that CISA does and the advisories that go out with numerous agencies' seals on them as a voice from the U.S. Government about what needs to be protected have a powerful message to our allies and to other entities looking for advice on what they need to patch and do in their systems. It's a critical function and it's something that CISA has made real strides in over the last several years.

Ms. Tokuda. Thank you.

Dr. Stewart?

Ms. Stewart. I agree, we do need these people to be working together to actually form an effective defense of these networks at the moment. Loss of knowledge that we've gained over a number of years will challenge how we coordinate and deploy in future on our abilities to deter these attacks, yes.

RPTR BRYANT

EDTR CRYSTAL

[10:12 a.m.]

Ms. Tokuda. Thank you.

And especially given the fact that many individuals that are in these roles that have been let go, the technical background, the on-the-job training that's required, the security clearance, the time it would take, what kind of a loss are we looking at to have to re-onboard these individuals, because clearly these roles are needed?

And, more importantly, Ms. Galante, you talked about the message it sends to our allies. What message is this sending to our adversaries?

Ms. Galante. This will be a significant blow to the people who have come in over the last several years or waited on clearances sometimes upwards of a year or more to come in for technically important roles where the training is limited on the outside and they're doing core work to secure U.S. networks.

This is a key issue that we need people to continue to come in, and we need the people who have been brought in to stay.

In terms of our allies, they rely on U.S. cybersecurity expertise in a way where they see movements from the U.S. as the leading posture for how they look to talk to their private sectors; and, in turn, that collective defense between governments that we're allies of and the private sectors that they inform help us keep our adversaries from further threatening U.S. networks.

Ms. Tokuda. Thank you.

And I know my time is running out now.

But to add on that in terms of our adversaries, I think, given recent conflicting reports about the administration suspending cyber operations against Russia and the clear alignment between the PRC and Russia, we need to consider how this could align in terms of both our cybersecurity threats and ultimately what are the risks of any failures to address Russia's threat and their cooperation and coordination with the PRC in terms of our cybersecurity and cyber vulnerability.

So if anyone has things to comment on that particular potential alignment of our adversaries?

Ms. Galante. China and Russia have been key cyber adversaries and cyber powers for over a decade at this point. Our ability and the U.S.' continued persistence to counter these adversaries in cyberspace is critical.

Ms. Tokuda. Thank you.

Anyone else want to comment?

Mr. Joyce. So I'd join.

There's been a common theme throughout this that we need aggressive actions to counter and deter. And it's very clear to me that unilaterally exiting the cyber battlefield would be a bad decision.

I don't know if we ever have it in that case, but I would hope we do not, because things like the defend forward strategy keeps not only the nation-state activity on their heels as we address their infrastructure, but it also undercuts their -- it undercuts their botnets and capabilities that are used by the criminals.

And so we're going to see, if we stop defending forward, we're going to see an increase in cybercriminal ransomware activity as well.

Ms. Tokuda. Thank you, Mr. Joyce.

And finally, I know that we have seen reports CISA has paused all work on related election security. Do you think China has stopped looking at potentially interfering with our elections through any kind of cyber attacks, yes or no?

Mr. Joyce. I have no reason to believe they have.

Ms. Tokuda. Thank you, Mr. Chair. I yield back.

Chairman Moolenaar. Thank you.

Representative Hinson.

Mrs. Hinson. Thank you, Mr. Chairman, and to our ranking member, for holding this hearing today. I've got to say I'm hoping that there are no AI videos of me like that out there. It's scary stuff.

We know AI has become such an incredible tool for so many of our small businesses, our farmers, schools, hospitals. It runs the gamut of who's actually using this technology for a positive purpose.

It's really, really important in a place like Iowa, where we can use that to really be a force multiplier for our businesses and our communities.

We're seeing it used increasingly in things like precision agriculture in farming and agriculture spaces. It helps to increase crop yields, which we've got produce more with less, conserve our resources, and then in that process also work to optimize all of our supply chains.

It's doing all that already. And so we're really leveraging that in a lot of really great ways. And we want all of our folks to have access to all these innovations and the technology, but we also have to protect them at the same time.

And I think that's a lot of what we're going to be focusing on this Congress, because, as we've heard today, it's the cyber threats, it's the data breaches, the operational disruptions potentially that could jeopardize success and security, especially, as we're hearing, that they may be advancing their own to be a peer-level capability.

So we know they're working in this space, that they're not a fair actor, and they're using these capabilities to steal, manipulate our markets, and continue to exploit the vulnerabilities in our critical infrastructure for strategic advantage.

Dr. Stewart, I want to go back to something you answered about earlier. You talked about some of the vulnerabilities in the designs for technology.

And as I was mentioning about all these folks who are using it, the farmers, the schools, hospitals, how can they really integrate these systems in place while ensuring that their data remains protected from the cyber threats, the malicious actors, especially given some of the challenges that many of our rural communities face with maybe affordability and access to these technologies?

Ms. Stewart. There's a number of very simple things that people can be doing to help secure those devices that they have.

Unfortunately, some of the devices just aren't securable, which is what we've really been talking about today.

But in making good choices on what equipment they're buying, things that have actually been certified to certain standards, not going, unfortunately, for the cheapest option is actually one of the best things people can do at this moment.

We have a number of incidents we've seen on things like solar installers, for example, asking people for their home passwords so that you can install the inverter and solar panel on your house.

Things like that we need the public to be aware of that they shouldn't be doing. Simple defensive techniques of, "No, you can't have my password. That's not a good idea."

Mrs. Hinson. Yeah. Good cyber hygiene across the board.

Ms. Stewart. Good cyber hygiene across the board, yes.

Mrs. Hinson. Yeah. I think about when someone comes to do maintenance at my house, I have a garage code that I can give them, but I can also change it and eliminate it as soon as I need to. Do we need something like that for that kind of situation?

Ms. Stewart. Eliminating things like fixed passwords in devices as a standard would be a huge thing that we could do to improve the technology and the security of that technology as well. It's really common on the edge devices at the moment.

Mrs. Hinson. Mr. Joyce, what proactive steps should the government be taking to protect our AI systems from cyber threats, unauthorized access, and additional data exposure?

Mr. Joyce. We are entering a new era with AI that will introduce new vulnerabilities. The most important thing is we've got to have the connection to both industry and academia that's looking at the new classes of vulnerabilities that are introduced by AI.

AI is going to make everyone faster, the attackers, the defenders. It's going to make everyone more capable. But it's also going to bring new classes of vulnerabilities that we don't appreciate yet.

And so that research and understanding, the adversarial testing of these systems, so that we break them before the Chinese or the Russians get to break them is going to be vital.

Mrs. Hinson. We've got to hack ourselves to figure out what we need to fix, right, almost?

Mr. Joyce. Exactly.

Mrs. Hinson. How critical is it to eliminate Chinese-made technology from our Federal infrastructure? We've already talked about Rip and Replace and why that program exists. But how critical is it? Is it a red lights are flashing alert? Do we need to do this yesterday? You all agree?

Mr. Joyce. Yeah. We've had programs talking about the threat of Huawei for years, and we've only just begun getting to the point where we're actually resourcing and taking action to get them out. But we're still binding the hands of some of our solutions.

For instance, HP Enterprises and Juniper tried to merge and create a capability that would be able to sell 5G solutions that are American made and have American software. It's so important to have the software be trusted from a trusted source.

And the Justice Department right now is looking at -- in fact they sued to stop the merger, which will undercut our ability to compete against Huawei in the whole global environment.

So we've got to get American businesses into the technology space and competing against the low-cost Chinese solutions.

Mrs. Hinson. We have to get ourselves out of our own way, in essence, get the government out of the way.

Mr. Joyce. Absolutely.

Mrs. Hinson. All right. Thank you, Mr Chair. I yield back.

Chairman Moolenaar. Thank you.

Representative Stanton.

Mr. Stanton. Thank you very much, Mr. Chairman.

Before I begin my discussion on this critically important topic today, all of us are reeling from hearing the sad news about the passing of our colleague Representative Sylvester Turner of Houston.

Congressman Turner, I was a mayor with him before I came to Congress. He's a legend of public service in Texas, having served in the legislature, as a very popular and successful mayor of the city of Houston, just beginning his career here in Congress.

And although he was only here a short time, he had a great impact on all of us.

And our deepest sympathies go to his family and to the people of Houston, a loss of a giant of public service in Texas.

I work hard to represent the very purple State of Arizona. I'm grateful to be here for my first hearing with the China Select Committee, one of Congress' most bipartisan committees. Protecting U.S. security has to be a bipartisan issue.

Unfortunately, this administration is harming decades of American soft power abroad and handing wins to our strategic competitors on a silver platter.

This administration dismantled USAID, a critical tool in countering the Belt and Road Initiative and the growing influence of the Chinese Communist Party. China is already stepping into the void that this administration is leaving.

I was heartened to find out this morning that the United States Supreme Court did block the dismantling of USAID and said that the congressionally approved budget that we approved in a bipartisan way has to move forward. It cannot be impounded by the President.

This administration has changed its position vis-à-vis Ukraine. The Ukrainian people are bravely defending their sovereign land against Russia aggression.

CCP leadership is watching and inevitably feels emboldened to reunite Taiwan with mainland China as a result of that change of policy by this administration.

Even ignoring our foreign aid, which is less than 1 percent of the budget, or aid to Ukraine, 70 percent of which was spent right here in the United States with American manufacturers, we are hurting our ability to stand against global threats.

DOGE has fired or driven out employees at the Cybersecurity and Infrastructure Security Agency, CISA, our primary cybersecurity agency.

In week one, he dissolved the Cyber Review Safety Board, a bipartisan board whose recommendations strengthened both public and private sector defenses. In fact, CSRB was in the middle of an investigation into Salt Typhoon, the Salt Typhoon hack into U.S. telecommunication systems, but the investigation had stopped when CSRB disappeared.

Ms. Galante, how might the administration's review of Federal grants and programs impact programs related to security telecommunication networks?

Ms. Galante. We need to fund these critical programs that help both secure and then in some cases even digitize rural areas in addition to underserved areas.

It's incredibly important that the cybersecurity programs that we have in place remain in place. CISA is a relatively new agency. The workforce there is building out a real ability to communicate with State, local, and other entities who have the tough job of really securing networks.

Whether it's that energy provider out in a local district or whether that's a company that's just looking for best practices, this is the way that a Federal agency is able to push those lessons and push that support out to the edge across the U.S.

Mr. Stanton. And what cybersecurity investments should we be making here at home? And what baseline standards should be put in place to defend against cyber attacks? A similar question to what you've answered already, but it bears repeating, please.

Ms. Galante. When you look to sectors across the U.S. that are the gold standard of security, you look to the financial institutions who have implemented cybersecurity programs that have a set of different elements that allow those institutions to give a deep understanding of baseline threats to their networks and to be able to flag when that activity is off.

We need that same theory behind the major programs that we have in key institutions for other critical infrastructure areas. Building that out and putting cybersecurity minimums in place in critical services, in critical infrastructure is a key goal for us to be able to secure U.S. infrastructure.

Mr. Stanton. Thank you.

Finally, Ms. Stewart, you mentioned in your testimony about the need to, quote, modernize and adapt grid technology, ensuring the U.S. power systems are secure from malicious intent.

That modernization would rely, in part, on semiconductors. Can you speak to the need for a diverse and secure semiconductor supply chain to protect our power grids?

Ms. Stewart. Yes. We can't necessarily build the components we need to secure our current supply chain. We don't have the manufacturer in this country at the moment. So actually building that base of supply chain coming and would enable U.S. companies to help assemble these components more securely as well.

That can be done quickly, but it does require funding support and coordination to get the right components and the secure designs in place.

Mr. Stanton. Thank you very much.

Mr. Chairman, I yield back.

Chairman Moolenaar. Thank you.

Representative Johnson.

Mr. Johnson. So I want to talk a little bit about LiDAR, Mr. Joyce. And when I raise concerns about how much control the Chinese companies have over the LiDAR market, I think some people wonder if the threats are really all that relevant to their life.

I came from the telecom sector, and it reminds me a little bit of how much of a foothold we let Huawei get into telecom networks.

So for an everyday citizen who wonders whether DJI drones or a tractor, a passenger vehicle with LiDAR is really that big of a problem, help us educate them.

Mr. Joyce. Congressman, LiDAR is not my area of expertise, but I certainly can talk to some of the supply chain and cyber threats.

The thing I worry most about is who controls the software underneath the capability. We can have trusted manufacturing in the U.S., but if the software is written inside the CCP and then beholden to Chinese intelligence laws, where it can be influenced, updated, and manipulated, that gives me grave concern.

And so where we don't have U.S. entities, whether it be in the core telecom options like we talked about in the Huawei -- in the competition against Huawei -- whether it be software that we would trust and install inside our clouds or inside our businesses, or all the way down to the edge devices we put in our home, who makes the software and who has the ability to update it is critical.

And so going to any component, whether it's LiDAR, drones, or others, that's my metric of security.

Mr. Johnson. So in your testimony you said we allow too many flaws in the software environment. We've had some discussion about that today.

But what are policymakers to do with that? It seems like perhaps a bit too aggressive to just say, "Oh, no, there can be no software written by any Chinese national or somebody living in China." What should policymakers do?

Mr. Joyce. I'm not sure that's not a reasonable outcome. I think the important thing is we have to have trust in the software and capabilities. It runs too much of our national security, too much of our economic security, and it's too embedded in our lives these days. So who makes that software is vitally important.

Mr. Johnson. So we'd want to make sure that our policies were able to hold up in court. And I know you're not a legal expert here opining on that.

Just from a practical operational perspective, would it be better to identify key strategic industries and niches whereby we would start to put up some of these safeguards first rather than something that's too blanket or too sweeping?

Mr. Joyce. Absolutely.

Mr. Johnson. I also am a little nervous in these areas where we have allowed Chinese companies to gain so much concentration in the market. Is there something -- in America, we don't do a lot of central planning. We generally are pretty resistant, as we should be, to industrial policy.

How should we view areas like Huawei or with drones or with LiDAR where China has been able to secure such an absolute domination in the market?

Ms. Stewart. A lot of the work I've done has been on the battery space essentially, which is one of the areas where China has completely dominated the market. And we're currently looking at how to improve that as well.

I do believe we can secure around that technology currently to enable us to continue its use, continue growth of our power, essentially, so we can still support things like data centers and the growth of the U.S. grid.

I do believe, though, we need to wrench back control from these companies as a whole. They hold power for things like contract controls, where these third-party companies have no power over if they can inspect the components they're importing or not, or, for example, we can inspect the components that they're importing as well.

We need to wrench that control power back into the U.S. so even if we are still importing PCs, we have control over contracts and the ability to inspect to see what's inside and to secure around those components to move forward while we build the U.S. supply chain for the future.

Mr. Johnson. So it does seem like wrenching back control -- I mean, I'm sure there are a variety of ways that could be done, but two come right to mind.

Number one, the ones you mentioned that talk about making sure we have almost an audit or a transparency into what's going on.

The other would be making it clear that the Department of Transportation or the Department of Defense or other American agencies should not be purchasing this software and entering into contracts with these entities.

Is that a reasonable policy approach?

Ms. Stewart. For some components, yes.

There are a number of components that we do not have a supply chain for currently in this country. And not having that supply chain will fundamentally impact our reliability in future if we do not build it quickly.

Mr. Johnson. Very good.

Mr. Chair, before I yield back, I just note I have a bill that would do just that with regard to LiDAR and Federal agencies and would urge you all to look at.

Thanks much.

Chairman Moolenaar. Thank you.

Representative Brown.

Ms. Brown. Thank you, Mr. Chair.

We are living in a time of escalating cyber warfare. Our foreign adversaries have been relentlessly attempting to breach U.S. systems, targeting critical infrastructure, government agencies, and private enterprises.

In addition to ensuing chaos and confusion, the underlying goal is to disrupt our national security, steal sensitive data, and weaken American institutions.

These threats underscore the urgent need for robust security measures to safeguard our Nation's digital infrastructure.

Cybersecurity is not just a technical concern. It is a matter of national security, economic stability, and public safety.

Without a strong and well-funded cybersecurity framework and workforce, the United States risks falling vulnerable to adversarial nations.

The Chinese Communist Party, Iran, and Russia are all seeking to exploit weaknesses in our digital defenses. This is why the recent efforts by the Trump administration and DOGE to reduce the number of government employees actively working on our cybersecurity defenses are not just misguided, they are dangerous.

Last month, President Trump fired 400 employees from the Department of Homeland Security, including over 130 cuts within the Cybersecurity and Infrastructure Security Agency, or CISA.

These are career employees who have worked to stand up an agency that Trump's own administration established during his first term and work to oversee all cyber risks among U.S. infrastructure, including our elections.

Beyond DHS, the National Science Foundation has already laid off 10 percent of its workforce, with potential cuts reaching 50 percent. NSF conducts vital research in cybersecurity and infrastructure, helping the U.S. stay competitive and protect critical systems.

Mr. Chairman, I ask to insert into the record a letter from a group of national security leaders, including former Secretary of Defense Chuck Hagel, expressing deep concerns that the layoffs and funding cuts specifically at the National Science Foundation will put the United States at a disadvantage when it comes to China's race to the top on global technology dominance.

Chairman Moolenaar. Without objection, it will be added to the hearing record.

[The information follows:]

******** COMMITTEE INSERT ********

Ms. Brown. Thank you.

These reductions threaten critical research that supports cybersecurity infrastructure resilience.

I know that our expert panel of witnesses here today understand the value of these agencies and the research they conduct because you've all cited them in your testimonies.

So I'd like to start with Mr. Joyce, but I welcome insights from any of our witnesses.

Can you discuss the role that agencies like CISA, NIST, and the FBI play in strengthening our Nation's cybersecurity and overall national security? And additionally, why is it critical that these agencies remain adequately funded and, at the very least, fully staffed and operational?

Mr. Joyce. Thank you.

All of the agencies you mention perform a critical role in our national defense, kind of as interlocking links in a chain that also goes out all the way into industry.

Critical infrastructure is often owned and operated by industry, but it's inside the government that we often have the classified understandings and the tools that are able to assist in some of the defense and deterrence activity.

I spent a career at NSA, and one of the things I was passionate about was bringing top talent into the government to work on these missions. And I will tell you right now, we are at a severe disadvantage with people believing that they can have a safe and secure career inside the government watching what's going on.

And so that's my concern, is, yes, there is an immediate issue with cuts, but the long-term concern is will the top talent come to work in places like we have served, because it may come at a cost.

Thank you.

Ms. Stewart. The Department of Energy is the one I have primarily worked with for the past 20 years. The work they do as a sector risk management, as well as CESER is the sector risk management for energy at the moment as well for electricity, they have primary points of contact with these utilities, with these entities that need to actually form the defense against some of the CCP entities as well. So if we don't have those points of contact, we will be at a fundamental disadvantage at this point.

They've built those relationships over a number of years. They are trusted to talk to these entities and help them on how to distinguish between, for example, the classified information, how to get that information to them, and then how to implement the defenses that we actually need.

We need to continue that. But losing those points of contact is a huge problem for us to actually be able to implement those defenses.

Ms. Brown. Thank you. My time is expired.

Chairman Moolenaar. Thank you.

Representative Bilirakis.

Mr. Bilirakis. Thank you. I appreciate it very much, Mr. Chairman, and I'm honored to serve on this committee.

So anyway, Mr. Joyce, on May 7, 2021, a ransomware attack on Colonial Pipeline captured headlines around the world, with pictures of snaking lines of cars at gas stations across the Eastern Seaboard and panicked Americans filling bags with fuel -- you brought this up earlier -- fearful of not being able to get to work or get their kids to school.

In Florida specifically -- I'm from the State -- our port and airport operations were severely impacted, both of which are critical to the economic health of my State.

Since China has so heavily prepositioned itself in our critical infrastructure, I shudder at the thought of such attacks across the country, let alone the current level of China's recent wave of cyber attacks.

Can you, sir, help me understand how China uses home routers, like TP-Link -- again, you brought this up -- to access our critical infrastructure in government agencies?

Mr. Joyce. Yes, Congressman.

The cyber operators inside China need to make a secure connection from China through to their victims, but along the way they want to shed their identity, they want to hide their origin as being from China.

And so along the way, there are tricks you can do to operate through others that you hack to break the links along the investigative chain to understand where you originate from.

And one of the tricks they do is they find vulnerabilities in these routers, the WiFi devices that are in our houses that are always connected, always on, and have high internet bandwidth.

And if they can hack those, they can bend their communications through your home, my home, and then on to their victim.

And that's the purpose and that's what they're seeking to do. And because of the protocols of the internet and its origins in academia and trust, we don't have the security built into the foundational layers of the internet that prevents you from lying about your point of origin and where your bits are coming from.

So it looks like the last hop that you arrived from, and that last hop is a trusted endpoint inside the U.S. And so those WiFi routers are the things that allow them to hide their operations at bulk and at scale.

Mr. Bilirakis. Thank you very much. I appreciate it.

Again for you, Mr. Joyce. That leads me to the Federal Acquisition Security Council established in 2018, which was established to identify supply chain risk management standards and guidelines. They have the authority to recommend exclusion or removal of covered articles, but to my knowledge they have not exercised that authority to this date.

I know that both Chair Moolenaar and the ranking member, my good friend Mr. Krishnamoorthi -- I'm working on that name, sir -- but he is such a good guy -- and I like the fact that you all work in a bipartisan fashion. We've got to keep that going in this committee, please.

So, again, the ranking member and the chairman worked last year on a bill to strengthen the FASC. But why do you feel the FASC has not made any recommendations, even with some of its organizational challenges?

Mr. Joyce. So, sir, I apologize, but I do not know why they're using or not using that authority.

Mr. Bilirakis. Anybody?

Okay. All right.

If you can look that up and get back to me, I'd really appreciate it. I think it's important.

I also serve on the Energy and Commerce Committee as subcommittee chair of the Commerce, Manufacturing, and Trade Subcommittee.

So how could the FASC work with the FCC and the Cyber Trust Mark program to create what could be the gold standard not only for the public sector but also for commercial entities, particularly involved in critical infrastructure? Do you have any recommendations on how these two programs could better be synchronized?

Mr. Joyce. I am not familiar enough with the programs.

Mr. Bilirakis. Okay.

Anyone else?

Ms. Stewart. The Cyber Trust Mark program has been a really interesting development for the edge devices that we look at as well. I work primarily, again, on things like inverters and grid devices.

There is a version of that program that was to look at these devices also from a safety standpoint. The UL listing on a lot of devices fundamentally did change how we look at safety over a number of years. People could see the UL listing marked on the device. And the home routers, for example, or home inverters, they could see that that device was certified to a certain level.

Our challenge is what level we certify it to for it to still remain safe and for it still to remain cyber secure but also affordable. So we really need to look at what level of that marking will work for these types of devices as well.

But that marking is very important for people that are looking easily to buy devices if when they see a mark that they can trust potentially from the U.S. Government, there is a lot they can do with that then to help improve this network as well. So the Cyber Trust Mark program has a lot of potential to help improve this.

Mr. Bilirakis. What about the third witness, do you wish to comment?

Okay, no problem.

Thank you very much.

And thank you again for allowing me to serve on this committee, Mr. Chairman.

Chairman Moolenaar. Thank you.

Mr. Bilirakis. I yield back.

Chairman Moolenaar. Representative Moulton.

Mr. Moulton. Thank you very much, Mr. Chairman.

And it's great to have you, Mr. Bil -- sorry, I'm still working on that name. Bilirakis.

Mr. Joyce, I notice that you served as acting Homeland Security Adviser under President Trump and also served on the National Security Council.

I just mention that because I think what you said about the current efforts of Musk and DOGE and how dangerous they can be to the future of the Federal workforce, not just the people we're firing haphazardly today, but the future workforce is really important.

I've already heard this anecdotally. I spoke at a college recently, and there were students who came up to me and said, "I wanted to serve in the government. I don't know if I should now."

I had two people, two friends of mine close enough to me to reach out for personal advice about whether or not to take the buyout offer. Both of them were parrying counter-offers on Wall Street.

These were the most talented people. The people who are taking the buyout offers are the people who have other options, not the people sitting in a corner office in the government wasting away.

So I have very serious concerns about the talent drain happening right now and the fact that we can't attract future talent if this is the way that we treat Federal workers. And I just want to say I really appreciate you bringing those concerns up.

You've also worked for a long time on both the government side of things but also now in the private sector. And I was curious if you think that DOD and CISA need to offer the private sector more in order to strengthen their cyber defenses and ability to respond.

How do we incentivize the private sector to do more when it's the private sector that controls so much of our infrastructure?

Mr. Joyce. Thank you, Congressman.

I do believe that the government relationship with industry is important. And I look back at the last three or four years and how far the connectivity has come, the conversations that happen, the advice, the free flow of information in both directions. That's got to continue to develop.

I do think that there are some important roles for government, though. Industry is often motivated by security. But in the end, just as we're talking about how TP-Link devices proliferate because they're the cheapest, there are economic decisions in industry made on cybersecurity.

And I think we have to look to the automotive industry. And the reason we have airbags and antilock brakes and seatbelts is not because eventually somebody saw the wisdom in doing that. In the end, we had to decide they were required for safety.

And there's probably some additional things that we have to do that are required for safety. And part of that is things like elimination of TP-Link, but other things are setting some standards for how devices are secured, how software is updated, and how we build the trust around things like multifactor identities.

Mr. Moulton. So you used the words "requirements" and "standards."

Mr. Chairman, I really hate to bring this up, but it sounds to me like he's talking about, dare I say, regulations, government regulations.

Now, I'm a Democrat who's not afraid to say there are a lot of places where government regulations go too far. But to simply strip them willy-nilly when we're seeing a clear issue here with companies not doing enough for their cybersecurity in ways that absolutely impact our national security, that's a real problem.

Specific to telecoms, because we've talked a lot about telecom hacking here with

Salt Typhoon, do you believe that the current regulations on telecom and other critical communications industries like that are sufficiently robust to protect against the national security threats that we face and that are increasing, especially from China and Russia?

Mr. Joyce. Yeah. I think in the telecommunications environment we are good with regulation. What I would encourage is that we look at the legacy devices inside that environment.

The need to keep backward compatibility for old, outdated protocols introduces some vulnerabilities. And the other piece is we just have to make sure that the devices we put in our infrastructure are secure and trusted.

Mr. Moulton. And how are we going to get the telecom companies to do that, to ensure that they're not putting in the cheapest alternative but actually the most robust systems that they can buy?

Mr. Joyce. I think we've made the first steps in that. They can't use Huawei in the core anymore.

And we're talking here about things like the edge devices where ISPs often -- I don't get to choose the router that comes from my cable company.

And so making sure that it's not the lowest-cost Huawei device, that's an important thing; that it's not a lowest-cost TP-Link device, that's an important thing.

So it's actions like that.

Mr. Moulton. Thank you, Mr. Chairman.

Chairman Moolenaar. Thank you.

Representative Moran.

Mr. Moran. Thank you, Mr. Chairman.

And thank you to each of our witnesses today.

This hearing should be deeply concerning and disturbing to every American, in my opinion.

As I'm listening to the testimony, though, I can't help but think back to the 2007 Bruce Willis thriller "Live Free or Die Hard."

And I think even back in 2007, if you've seen that movie, a lot of what you're talking about here actually came out in that theatrical performance, which is incredible to me that we're 20 years down the road and we're still not prepared really for the cyber attacks on our domestic infrastructure, what was termed in that movie to be a fire sale.

And so that's really concerning. It should be concerning to our national security interests here in the United States.

Mr. Joyce, I want to start with you.

Just last week CrowdStrike released a report that there was a 150 percent surge in espionage attacks, with critical industries seeing up to 300 percent spike in targeted attacks. In particular, they highlighted that China's cybersecurity espionage has been accomplished by developments in their generative AI.

You stated earlier that -- I think this was your quote -- "We don't use all the tools that are available to us." And so my first question to you is, what tools are we not using that we need to be using to push back?

Mr. Joyce. Thank you, Congressman.

I've raised a few of them. I do believe that we can streamline the authorities and the capabilities that allow us decisive action in cyberspace, remove the policies that make it hard to coordinate the pushback, the takedown of botnets.

I watched the work that Cyber Command and FBI do to take down botnets that are used by both nation-states and criminal activities, and they to a great extent are able to disrupt these botnets. But I watch the amount of bureaucracy it takes to get all the authorities and to align the approvals to do and undertake those authorities, and we're just not as agile as the cyber attackers. So that's one thing.

The second is thinking about how do we mount pressure on the PRC in ways that it hurts, or other countries like Russia, Iran, North Korea, that it hurts, right, using the elements of sanctions and diplomacy.

And I was serious. I will be convinced that we're using more of our tools when I see diplomatic expulsions over cyber events, because we don't do that at all today.

Mr. Moran. Yeah. And you were talking about sanctions and diplomacy in both sides of the aisle today. Both Democrats and Republicans have talked about going on the offensive. And I'm going to tell you, I'll echo and join the call of Ranking Member Krishnamoorthi to hack the hackers and target those individuals who are targeting the United States and our citizens.

I think that's imperative that they feel the pain and that they know that there are going to be direct and swift and severe consequences to cyber attacks against the United States and its citizens.

Ms. Galante, I want to ask you, we know the PRC is not operating alone, as has been discussed today several times. They're using private entities in their own country to conduct these espionage and cyber attack efforts.

Do you agree with the fact that we need to go on the offensive more, one? And then can you also elaborate a little bit more about how the Chinese state is using these entities?

Ms. Galante. Yes. We need to continue to stay on the offensive against the companies that enable the PRC, China's state cyber operations.

The way that we can go after these companies, we have to have a faster response to be able to identify them and identify the key people who are building the tools that are used to exploit U.S. networks.

The level of granularity that we have on how the state services in China, the intelligence service in China tasks out and buys tools that are used against American networks specifically and explicitly is incredibly important to stop.

This will take a large effort. This is not a small group of companies. It's an ecosystem around a town called Chengdu, a city called Chengdu.

This is a well-known group of people who started in the late nineties under what was then called the Green Army. Like, these are longtime highly expert professionals in cybersecurity and IT who are being used, whose tools are being used to go after the U.S.

We have to deter that activity going towards U.S. networks.

Mr. Moran. And, Dr. Stewart, I'm going to come to you with the last question, because we're talking about people. And you mentioned earlier what we really need is more people in the United States that are involved in this industry, cybersecurity industry, that can help us.

How do we attract the best of the best, not just to be educated and learned in this area, then go to the private sector, but also to be in the public sector, in government, to fight back on an intelligence and cybersecurity level? How do we recruit and retain those individuals to work for us in our national security and intelligence sectors?

Ms. Stewart. I will add I don't think we necessarily just need cyber people. We also need engineers that can help build the controls around these systems better for us for the future as well.

I think we need to build from a foundation of better education for people to come into engineering and cybersecurity careers, even beginning from high school at this point, to understand the actual importance of this technology.

It's not just going in to work for a startup or doing that kind of work as well. They can go work for utilities and help keep the lights on every day.

That mission is something I've done my entire career, and it inspires me every day.

But we need to be able to keep that building and help tell people there are jobs and careers and salaries that can help them sustain a life here as well. So we need to encourage people into this industry even from the beginning of high school at this point.

Mr. Moran. Thank you all.

Mr. Chairman, in conclusion, I'll say in this particular instance I think a great defense means a really good offense. We need to go on the offensive.

Thank you. I yield back.

Chairman Moolenaar. Thank you.

Representative Stevens.

Ms. Stevens. Thank you, Mr. Chair. And thank you for this very important hearing where I feel as though not only the testimonies but the questions that have been asked are moving the ball forward and not only uncovering but helping us to identify more areas of policy consideration.

Of course, maybe I'm biased that my chair also hales from the great State of Michigan and is exactly where he's meant to be in terms of leading this important committee.

But many of you know that since 2016, the National Institute of Standards and Technology, NIST, is a foundational agency in developing new cybersecurity standards. I even had the privilege of working with NIST in my pre-elected life on the cybersecurity standards.

And they have been supporting the creation of post-quantum cryptography, PQC. And in August 2024, NIST unveiled the world's first PQC standards, which were met with widespread acclaim.

However, both public and private sector entities haven't really been able to get to the steps, the necessary steps to prepare for this quantum/post-quantum era. And given the last major encryption standard update that it took 7 to 10 years to implement, I'm kind of growing concerned that the U.S. might be vulnerable in this post-quantum world.

So, Mr. Joyce, from your perspective, what are the primary barriers preventing both government and private sector entities from adequately preparing for PQC, post-quantum cryptography, and how can Congress assist in overcoming those challenges?

Mr. Joyce. Thank you.

I agree that business and industry as well as government need to focus on the transition to quantum-resistant encryption. NIST did a good job of accelerating the standards-making process and communicating what is adequate standards against a quantum computer, the threat from a quantum computer.

The biggest thing people need to do today is they need to start to understand where we use encryption and vulnerable protocols inside the ecosystem.

So the biggest companies, the hyperscale cloud providers, like Google and Microsoft and Amazon, have already started their journey to experiment with the algorithms and to put them into the ecosystem.

The next big step is businesses and government need to start inventorying where we use those encryption technologies.

And it is not just the privacy of our data, but the authentication systems used throughout the ecosystem also rely on some of those vulnerable algorithms. And so we've got to have an understanding of where they are in the ecosystem.

It's then with that understanding that you can start the programs to replace and build in the agility to swap in new algorithms.

So you don't want to just take out one old algorithm, put in the new one. You want to build in the infrastructure that lets you continue updating encryption as we learn about new threats.

Ms. Stevens. And what's the incentive to do that? Would that be coming from us, a directive? Is it a certain agency that could be working outside of -- I mean, in addition to NIST? I mean, they're not necessarily regulatory. They're more of a public-private partnership type model, the humble agency that does a lot with very little, but --

Mr. Joyce. Yes. So on the government side, the direction's already there. There is a Presidential executive order requiring quantum-resistant capabilities I think 2034. And it's also been enacted in the NDAA through Congress. So there is --

Ms. Stevens. NDAA is a great vehicle.

And then, Dr. Stewart, given the substantial differences we face simply preparing private entities with critical infrastructure for cyber threats from classical computing to the like, what steps should Congress take to assist organizations, some of which may not fully understand what quantum computing is or entails, to defend against emerging threats?

It was great to hear about the hyperscale cloud from Mr. Joyce, but I would love some more thoughts from you, Dr. Stewart.

Ms. Stewart. From the operational technology side, there's a number of our components and devices that don't use encryption and can't use encryption for them to operate safely and secure -- well, safely.

We just can't use encryption for that. We need better things to secure around those components, and we can't use encryption in many of the commons or PLCs and other controlling devices, because it will damage our ability to safely operate them as well.

So we need to also consider when we talk about standards for things like this where the right places to apply are so people can actually prioritize that in their systems. If there's a standard written and we tell these entities they need to do it, some of them may spend that time hunting down the thing that they can't actually do to begin with.

Ms. Stevens. Is there an investment challenge too on that front -- I mean, a monetary challenge?

Ms. Stewart. Yes. Providing funding also to those entities to help improve their security is important, and continuing to provide that funding from Federal programs also.

Ms. Stevens. I used to call that the digital manufacturing assistance program.

With that, Mr. Chair, I'll yield back. Thank you.

Chairman Moolenaar. Thank you.

Representative Newhouse.

Mr. Newhouse. Thank you, Mr. Chairman.

Could I ask one question of the chairman? Do we know for sure if the Raj, the ranking member, was the real one or the AI-generated one?

Chairman Moolenaar. We believe he was the real one.

Mr. Newhouse. Okay. Could you look into that for us?

Well, thanks to the witnesses for being here and having this very important conversation that we need to understand as a country much better.

We know that the U.S. intelligence community assesses that the PRC is the most active and persistent cyber threat to the U.S. PRC cyber threat actors are known to conduct economic espionage and intelligence-gathering operations.

Throughout the last couple years, that has shifted targeting to U.S. critical infrastructure entities with disruptive cyber capabilities.

So due to the interconnectedness of all U.S. critical infrastructure sectors, impacts in these areas certainly could affect many things -- our supply chains, our business operations, our civilian life -- and certainly could delay the response of U.S. military personnel.

In my district in central Washington State, we have the Pacific Northwest National Laboratory, just not to be one-upped by Idaho National Laboratory. But I certainly understand the important role that labs play in this area, and I have a deep appreciation for labs that have truly been called the jewels, the crown jewels of our Nation as it relates to research and innovation.

Dr. Stewart, thanks for being here.

In your testimony, you talk about electricity as being the fundamental source of stability and economic prosperity, and I certainly agree with that premise.

As you know, in the Pacific Northwest we are blessed to have a proven reliable resource of electricity, baseload electricity and hydropower in our river systems, which provides us 90 percent of our region's electricity.

And it struck me after reading some of your testimony that efforts that we've seen recently to remove some of the dams that we have in our region would not only threaten our livelihood in the Pacific Northwest but could hamper our ability to respond to electricity demand, and that would have tremendous terrible effects.

I just wanted to get your thoughts on whether you could elaborate for the committee a little bit on the importance of addressing the highest consequence in most critical sites, as well as incentivizing the strategic repatriation of a technology.

You talked about Rip and Replace, I believe, and how important that is, the hardware, the firmware, the software, how important that replacement and improvement is.

Ms. Stewart. So cyber-informed engineering is one of the techniques we've been using to help produce those consequences.

I believe fully that when cyber teams and engineering teams actually work together and are able to evaluate what the highest consequence truly is from the system, they are able to come up with not just cyber mitigations but engineering mitigations that may prevent the fire, the lights going out, the water pump stopping.

Those aren't always cyber-related, and they have to work together to be able to understand what they are mitigating at the same time.

One of the big examples we might have is loss of comms on devices doesn't always mean the lights might turn out as well.

So, strategically, being able to lose communications from a device but keep the lights on is a really important feature for a lot of our work, especially if we can maintain safety at the same time as well.

That's one of the things from Colonial Pipeline, for example, that's a very good example. If they could have safely been able to engineer and operate those pumps and that pipeline from the OT side without worrying about their IT or their billing, they would have been able to continue operations. We wouldn't have had that worst case scenario of losing the gas pipeline at the time.

So it's really important that we build in those engineering mitigations, working with the teams together. We also need the people that are both engineers and cyber teams to work together on that responsibility as well.

Mr. Newhouse. Very good. Thank you. Thank you.

Ms. Galante, just to build on what has already been discussed, do you see a viable diplomatic option to deter China from the kind of activities?

And if so, could you detail it for us? And do you believe that the Cyber Mission

Force structure is adequate for defending our country against this kind of cyber activity?

Ms. Galante. We need to counter-trend the cyber aggression on a variety of fronts. That includes diplomatic.

There is no one silver bullet in how we're able to deter China. To date, a broad swathe of efforts have put some level of friction into the gears of how some of the Chinese operators work. That has been able to shift their motives. It's also shifted some of their targeting.

But the point that we're at here in 2025 is we have prepositioned assets by the PLA, by the Chinese military, across critical infrastructure, and we also have a massive cyber espionage operation against the telecoms.

Being able to use the full set of discussions, tools, and state tradecraft to message to China and to hold consequences against China that this is unacceptable and it's unacceptable against America is critical.

Creativity in how we're able to link these cyber operations to other punitive measures that we take against China is a key way to make that message stick.

Mr. Newhouse. Great. Thank you very much.

Again, thanks to all of the witnesses.

Mr. Chairman, I yield back.

Chairman Moolenaar. Thank you.

Representative Torres.

Mr. Torres. Thank you, Mr. Chairman.

The PRC has prepositioned itself in America's critical infrastructure not merely with an eye toward espionage but with an eye toward sabotage, which represents a new escalation in the ongoing cyber conflict between the United States and China.

Volt Typhoon is designed to have the deterrent effect of a gun pointed squarely at the head of the United States with the CCP's finger on the trigger.

Mr. Joyce, what are the likely provocations that would trigger Volt Typhoon cyber sabotage of America's critical infrastructure? Is it all about deterring the United States from halting or impeding an invasion of Taiwan? To your knowledge, what is the CCP thinking?

Mr. Joyce. Congressman, I don't think it's aimed at deterring. I think it is intended to be an operational tool at a time of escalating tensions to get us to turn inward and not focus on supporting operations in their theater.

You know, I used, in my opening statement, I used the word "terrorism." I didn't use that lightly. If you think about the idea that they want societal panic, they want us worried, angry, afraid because things are happening to our critical infrastructure, that is terrorism. They intend to inflict terror, and that's deeply concerning.

Mr. Torres. And I could be wrong here, but the United States is presumably in China's critical infrastructure and China is presumably in ours.

Is the dynamic between the United States and China simply one of mutually assured destruction? Like, is there an analogy between cyber deterrence and nuclear deterrence? Or am I thinking about it incorrectly?

Mr. Joyce. I don't think cyber force stops cyber force or other actions independently. I think it is one of many tools.

So, for instance we heard about the successes and we've talked about them throughout today, about getting into our critical infrastructure. And none of us here said, "Oh, they have an advantage, we're going to curl up and go away." It increased our resolve. It was escalatory.

I do think that we are a rule of law country and we operate differently. Under international -- under the law of armed conflict, we can't inflict pain just across the population of another country. It simply is against international law.

So in the U.S., we wouldn't go broadly take out a water supply, an electric supply. So I don't think we are on equal footings, because we're not seeking to deter to the Chinese population. We're looking to deter the PRC, though.

Mr. Torres. Former Director of the FBI Christopher Wray testified that even if all of the FBI's cyber resources were focused exclusively on China, the cyber personnel of China would nonetheless outnumber that of the United States by a ratio of 50 to 1.

So we know that China has an overwhelming quantitative advantage over the United States in a cyber conflict. Does China have any qualitative advantages over the United States?

Mr. Joyce. They are certainly improving rapidly.

Mr. Torres. Or to put it differently, who is the cyber superpower of the world? Is it the United States or China?

Mr. Joyce. We still are the cyber superpower, but that gap has closed dramatically in recent years.

Mr. Torres. The central government of China controls 100 percent of its critical infrastructure, whereas the Federal Government of the United States only controls a fraction of its critical infrastructure.

And the United States' ownership of critical infrastructure is broadly distributed. For example, the United States has 50,000 water systems that are largely run by the smallest localities or utilities with the most minimal resources.

We're powerless against a well-resourced nation-state like the PRC.

Ms. Galante, is the diffuse ownership and operation of American critical infrastructure an insurmountable advantage in our Nation's cyber conflict with China?

RPTR MCGHEE

EDTR CRYSTAL

[11:10 a.m.]

Ms. Galante. It certainly requires an approach of more people focused across the U.S. on upping the basic cybersecurity of many of these operational technology systems. Every water municipality, for example, is run differently than the one a few counties over.

Looking for how you secure the devices, the architecture and the buildouts of these systems requires expertise that we're desperately in need of in this country and the cyber workforce we need to continue to build.

Mr. Torres. I see my time is about to expire. Thank you.

Mr. Moolenaar. Thank you.

Representative Nunn.

Mr. Nunn. Well, thank you, Mr. Chairman.

Thank you for the members of the panel for being here today.

Chairman, I think you state correctly here, the United States is currently under attack by the Chinese Communist Party, particularly through its cyber operations currently underway.

China's offensive hacking capabilities are larger than that of every other nation combined -- Salt Typhoon, Volt Typhoon, Silk Typhoon, Flax Typhoon. It's clear these operations are nefarious and they are coordinated, as evidenced by the work of this committee and the intelligence community members who are here today.

Thank you.

We know that China has infiltrated our critical infrastructure and attacked our key telecommunications.

I believe that the U.S. must end our era of reactionism and platitudinal defense. We must pursue a new approach rooted in deterrence and holding bad actors accountable.

Look, I'm a former counterintelligence officer who's worked in China. You have all done your job. You've seen the adversary front on.

I served as the director of cybersecurity at the National Security Council, and this has been an evolving threat, but it is one that we have not even begun to deter in an effective way.

I believe that while traditional forces in our military prepare for a kinetic response in cyber, we must be more adaptable. We must be able to operate where the CCP has been operating every day.

Mr. Joyce, your arguments, I think, are effective. We must be able to operate offensive cyber operations, disrupt their capabilities, target economic sanctions must be part of the toolkit here, public indictment, coordinated international law enforcement actions, diplomatic pressure, export controls, intelligence sharing. The list goes on. The challenge is the actions have not followed suit.

I believe that we must have a whole-of-government response, and I hope that this administration is prepared to stand up to China in a bipartisan way.

So let's get started with this.

Director Galante, you were the cyber executive director for cyber threat intelligence integration at ODNI. We both served there together. Thank you very much for your service on this.

I want to be very specific here. Did the Chinese Ministry of State Security coordinate the Typhoon attacks?

Ms. Galante. They directed them through a contractor.

Mr. Nunn. Did the MSS coordinate attacks that impacted both President Trump and at the time candidate Kamala Harris?

Ms. Galante. There's reporting of that, public reporting.

Mr. Nunn. At the unclass level, do we believe that they were the ones behind the assault on our nine largest telcos?

Ms. Galante. Salt Typhoon is the group associated with the MSS and the contractors behind this activity.

Mr. Nunn. Did the MSS also direct attacks on our Department of Treasury just this year?

Ms. Galante. Yes.

Mr. Nunn. Did every American citizen who uses one of those telcos become a target of the MSS with their operation?

Ms. Galante. They had the ability to go after a variety of subscribers to these different telcos.

Mr. Nunn. So from the President down to everyday American citizens, the MSS is casting a wide net.

Can you talk to me about, at a top level, have you seen a response that would deter the MSS at this point?

Ms. Galante. The response is beginning, but at this point this activity continues, and over the last several years more offensive espionage collection efforts, in addition to offensive prepositioning efforts, have occurred.

Mr. Nunn. I want to highlight the chart behind me here.

Look, there are ways that we know the MSS operates.

First and foremost, did any of these actors, unlike what maybe Russia would do, is say a cyber criminal element did this, do we think that any of these actors within China are operating autonomously, or is the MSS directing and giving them a cyber target to go after?

Ms. Galante. I don't know the actors directly behind you, but generally, the actors within China, within their contracting ecosystem, are directed by and are paid by the MSS and in some cases the PLA.

Mr. Nunn. So no one is doing this rogue. This is a coordinated effort by top leaders within the MSS.

Ms. Galante. Yes.

Mr. Nunn. The actors behind me identify one of the last cyber attacks. Now, the FBI sent out warrants. We've identified them. There is a clear command-and-control structure within the MSS. And I would argue that one of the best ways to go after this is to go after top leadership rather than just the defensive operations that we've done.

Mr. Joyce, in our remaining moments here, what would be some of the top things that the U.S. can do to hold MSS actors accountable?

Mr. Joyce. So, first, I think it's a mindset, and the committee today is putting a stark spotlight on that. Imagine, if you will, we found the Chinese intelligence service prepositioning Semtex explosives in our ports and on our pipelines. We wouldn't tolerate that, right?

Mr. Nunn. Right.

Mr. Joyce. We would respond. And I don't see us responding with the force and the vigor, with all elements of the government capabilities, like they have prepositioned explosives on our infrastructure. And that, in effect, is what they have done.

So it is the increase and focus across all of the elements you mentioned, resourcing them and getting behind, pushing back, so there are real consequences each time we catch them doing this.

Mr. Nunn. Thank you, Mr. Joyce.

Thank you, Mr. Chair. I yield my time back.

Appreciate the panel.

Mr. Moolenaar. Thank you.

Representative Kim.

Mrs. Kim. Thank you, Chairman Moolenaar, for holding today's hearing.

And I want to thank all the witnesses for joining us today and staying until the end.

It's evident that the CCP has demonstrated time and time again a willingness to conduct potentially disruptive cyber attacks on our infrastructure.

In 2004 PLA-affiliated hackers infiltrated the systems of at least two dozen critical U.S. entities while cyber attacks against Taiwan doubled, with over 900 cyber attacks targeting Taiwan's government and private sectors.

Mr. Joyce, what should be the U.S. cybersecurity strategy's top priority? Is it the detection of these offensive cyber operations, mitigation, or on implementation of defensive measures?

Mr. Joyce. Thank you, Representative Kim.

I really do believe it's a three-legged stool.

One is the deterrence actions we've been talking about.

The second is improving the defenses so they don't succeed nearly as often.

And the third Dr. Stewart talked about is resilience activity, is making sure that even in the event somebody succeeds that there are manual backups, there are processes that we're able to fight through a cyber attack and continue to provide the services that are being threatened in cyber space.

Mrs. Kim. Thank you.

Ms. Galante, how can we work better with our allies and partners, like the Five Eyes, to counter the CCP's malicious cyber operations?

Ms. Galante. There are a number of allies in East Asia and South Asia who are interested in working with us and have a common interest in detecting Chinese activity on their networks.

The Indians, the Philippines especially have the tools but need additional capabilities to be able to find this activity.

They look to the U.S. as a partner and a provider for the types of intelligence sharing that will be key for these countries to be able to find that activity and also share it with their private sectors.

Mrs. Kim. Let me also follow up with Dr. Stewart.

What steps should Congress take to strengthen the critical infrastructure and reduce the supply chain vulnerabilities that are exploited by campaigns like the Salt Typhoon?

Ms. Stewart. A couple of things.

I mentioned that I believe we do need to have a strategic unity of force. You mentioned prioritizing between things, between offensive and defensive actions.

I believe we need all of these, honestly, and confirmed between all of us that we are coordinating across all the different entities, agencies, and abilities to deploy.

That includes things like there are volunteer entities that are attempting to help the infrastructure as well to put in those controls, helping them to remediate the vulnerabilities that still sit there on the systems and the legacy equipment that we're talking about today.

Coordinating between those entities would be an excellent way to help show the force that we have so it wouldn't just be we have the FBI or we have CISA. We have everyone who's able to coordinate doing that so that we're both efficient and able to get those solutions out there in place.

Mrs. Kim. Thank you.

We've heard multiple times in this committee about the breadth of PRC targets and the depth of access in various sectors.

So can you talk to us about the tools that we should be prioritizing on deterrence to mitigate our vulnerabilities.

Ms. Stewart. At the very simplest level, I believe we shouldn't make it easy. There's lots of devices and items that are just sitting on the internet that shouldn't be there as well. There's some very basic things that we are just not getting right in lots of places, and we have to.

Mrs. Kim. Do you think sanctions are particularly effective?

Ms. Stewart. Yes, I believe sanctions are effective to get people out of our networks and encouraging them onto the easiest spaces, but if we still keep making it easy from the infrastructure perspective, then it will never deter even with sanctions in place as well.

Mrs. Kim. Are the current international legal frameworks responsive to counter cyber operations?

Ms. Stewart. I do not have an answer to that, but I can prepare one for you.

Mrs. Kim. Does anyone want to cover that?

Mr. Joyce. So I think it's very evidently not adequate.

When hackers can come from Russia, China, other denied areas that don't participate in international law enforcement, that gives safe havens where they get to keep taking shots on goal. They keep coming at us from these places. And they know that they're beyond the reach of Western law enforcement.

Mrs. Kim. Well, quickly, what are some of the ways we can change the CCP's aggressive offensive cyber operations behavior? Three seconds left. Four seconds left.

Ms. Galante. I think we need to tie the cyber activities that are unacceptable that the PLA and the PRC do to other actions that we take outside of the cyber domain against China.

Mrs. Kim. Thank you.

Thank you, Chairman. My time is over.

Mr. Moolenaar. Thank you.

And I want to thank all our witnesses today. This is a very informative hearing and we really appreciate your participation and your expertise.

Questions for the record are due one week from today.

And without objection, the committee hearing is adjourned.

[Whereupon, at 11:23 a.m., the select committee was adjourned.]